статья предлагает один из множества способов их комбинации для обеспечения информационной безопасности, а в частности, определения уровня защищенности «произвольной ИС» и проведения работ по увеличению показателя защищенности этой ИС.

УДК 342.922/951

П. А. Криворотова
Научный руководитель: ст. преп. В. М. Жернова
Южно-Уральский государственный университет, Челябинск

ОБЗОР НОРМАТИВНО-ПРАВОВОЙ БАЗЫ В СФЕРЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье проводится обзор и анализ нормативных правовых документов, которые регламентируют деятельность по обеспечению безопасности критической информационной инфраструктуры Российской Федерации. Применение исторического метода в исследовании позволило провести анализ развития и создания системы ГосСОПКА.

Ключевые слова: критическая информационная инфраструктура; безопасность объектов.

Каждый год средства массовой информации публикуют все больше сообщений о кибератаках на объекты критической информационной структуры коммерческих компаний и государственных организаций. В ответ на угрозы было решено спроектировать и ввести в эксплуатацию государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

В 2013 г. Указом президента РФ от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [1] было постановлено возложить на Федеральную службу безопасности полномочия органа исполнительной власти по созданию системы ГосСОПКА.

Следующим шагом было утверждение Концепции № К 1274 12 декабря 2014 г. [2], в которой более конкретно определяются виды обеспечения, необходимые для ее создания и функционирования. В концепции был увеличен перечень осуществляемых системой функций, а также ее территориальная и отра-

слевая организация. В составе системы также функционирует Национальный координационный центр по компьютерным инцидентам (НКЦКИ), созданный в ФСБ.

12 июля 2017 г. Государственная дума приняла во втором чтении Закон «О безопасности критической информационной инфраструктуры» [3]. Он вступает в силу с 1 января 2018 г. Настоящий федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации <…> «в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак», — говорится в документе. В нем описана система, представляющая собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Основные функции системы состоят в том, что она должна представлять собой совокупность отечественных программно-технических средств с максимальным уровнем защиты, сформировать единое информационное пространство, позволяющее осуществлять оперативный контроль и защиту объектов критической инфраструктуры (атомные и гидроэлектростанции, системы снабжения городов и спецхранилища Росрезерва и т. д.).

ГосСОПКА будет проводить мониторинг электронных ресурсов, выявлять и прогнозировать возникновение угроз, а также совершенствовать существующие системы безопасности, взаимодействуя в том числе с операторами связи и интернет провайдерами.

Согласно Доктрине информационной безопасности, основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются в том числе «повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры», что является непосредственными задачами федеральной службы по техническому и экспортному контролю (ФСТЭК) в части технической защиты информации [4].

Так, согласно нормативным документам, определяющим создание и развитие системы, в сферу регулирования ФСТЭК будут входить задачи по защите от атак отдельных информационных систем, надзор за выполнением требований, определение набора средств защиты в составе информационных систем.

После утверждения законов и переходя к практике создания системы ГосСОПКА по указу президента № 31 ФСБ начала разработку собственного

программного обеспечения, нацеленного на обнаружение и предупреждение компьютерных атак [5]. Для отладки разработанного программного обеспечения ФСБ запросила у объектов критической структуры образцы их трафика за определенное время. На этих образцах будет проводиться проверка компетентности функционирования разработанного программного обеспечения. Его функция состоит в анализе трафика на предмет сигнатур вредоносных программ и дальнейшее информирование ФСБ и работников критически важных объектов о возможных угрозах и способах их устранения.

К январю 2018 г. ФСБ планирует ввести данное программное обеспечение в эксплуатацию на выбранных объектах критической структуры. Для этого объекты обязаны приобрести специальную компьютерную технику, обладающую необходимой производительной мощностью для обработки используемого трафика. Далее каждый критически важный объект должен купить лицензию на использование разработанного ФСБ программного обеспечения и установить его на приобретенной компьютерной технике.

В ноябре 2018 г. каждый объект критической инфраструктуры обязан завершить работы по установке системы и начать ее фактическую эксплуатацию.

ГосСОПКА будет функционировать с помощью программного обеспечения и ФСБ. ФСБ будет исследовать трафик, находить в нем вредоносные программы, устанавливать их причины, контролировать степени защищенности секретных данных и информировать объекты о возможных атаках.

Подводя итог, можно сказать, что информационная безопасность государства зависит от многих факторов [6]; проведена огромная работа по созданию нормативных актов, разработке и организации единой упорядоченной структуры по защите ключевых объектов нашей страны от компьютерных атак системы, которая отражает общемировую тенденцию по увеличению роли государства в обеспечении национальной безопасности.

Список литературы

1. Указ Президента РФ от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Собрание законодательства РФ. 21.01.2013. № 3. Ст. 178

2. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274.

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Рос. газета. № 167. 31.07.2017.

4. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: http://kremlin.ru/acts/bank/41460.

5. Указ Президента РФ от 23.01.2015 № 31 «О дополнительных мерах по противодействию незаконному обороту промышленной продукции» // Собрание законодательства РФ. 26.01.2015. № 4. Ст. 643.

6. *Кузнецов П. У.* Отдельные аспекты формирования правового обеспечения международной информационной безопасности // Вестн. УрФО. 2016. № 4 (22). С. 38–43.

УДК 34.03

Я. В. Кузьмина
Научный руководитель: д-р тех. наук, проф. В. Л. Кузнецов
Московский государственный технический университет
гражданской авиации, Москва

ПРАВОВАЯ СИСТЕМА ПРОТИВОДЕЙСТВИЯ ЭКОНОМИЧЕСКИМ ПРЕСТУПЛЕНИЯМ

Аннотация. Данная работа представляет собой аналитический обзор основных современных правовых актов в области экономической безопасности. Целью работы является выявление взаимосвязей между действующими правовыми актами и рекомендациями по порядку их применения на основе существующих практик. Актуальность работы определяется неуклонным ростом процентного соотношения числа экономических преступлений к преступлениям в других областях, а также стремительными изменениями технологий и программных продуктов, связанных с обработкой экономической информации, приводящих к необходимости совершенствования правовых актов.

Ключевые слова: экономическое преступление; ответственность; кодекс; экономика; законодательный акт.

Активная правотворческая деятельность государства в экономической сфере вызывает ответную реакцию населения: начинает складываться теневой сектор экономики, что толкает государство на ужесточение санкций.

Уголовный кодекс Российской Федерации (УК РФ) 1996 г. определил ответственность за преступления в сфере экономики в разделе VIII, состоящем из трех глав — 21–23 [1].